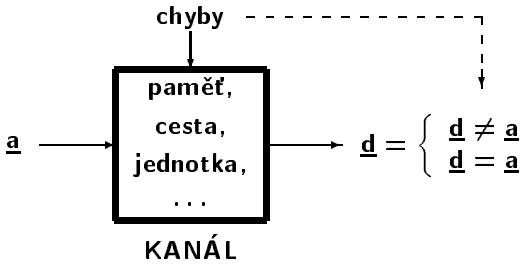
BEZPEČNOSTNÍ KÓDY



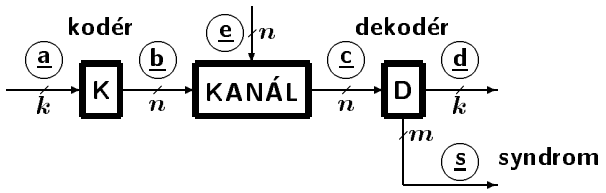
modely kanálů (charakter chyb):

kanál • symetrický: pravd(0→1)=pravd(1→0)
- ◦ nesymetrický: $\neq$
- ◦ s výmazem

kanál • bez paměti — „nezávislé“ chyby
- • s pamětí — shluky chyb

Př.: a = 1110 1111
d = 1011 0111
↓ ↓ ↓
0101 1000
a ⊕ d

{ 3 chyby nebo
1 shluk délky 4 anebo
2 shluky délky 1 a 2



a = $(a_1, \ldots, a_k)$
b = $(b_1, \ldots, b_n)$ slovo, vektor, znak, ...
⋮
slova { kódová, nekódová, nebo znaky { přípustné, nepřípustné.

ozn.: $B = \{\text{kódová slova}\}$
kód $\mathcal{K}$: a→b
!!! někdy pouze B !!!

Př.:

	b			
a	$\mathcal{K}_1$	$\mathcal{K}_2$	$\mathcal{K}_3$	
0 0	0 0 0	1 1 1	0 0 0 0 0	α
0 1	0 1 1	0 0 1	0 1 0 1 1	β
1 0	1 0 1	0 1 0	1 0 1 0 1	γ
1 1	1 1 0	1 0 0	1 1 1 1 0	δ

dvojkový kód: $b_i \in \{0, 1\}$
blokový kód (n,k) — určeno n a k
k informační (rozhodovací) obsah, míra informace, informační entropie } shannon (nespr. bit)
$m = n-k$ redundance, nadbytečnost
k/n norma kódu, přenosová rychlost, poměrná (relativní) míra informace } %
m/n poměrná (relativní) redundance

systematický kód: slovo { informační část, kontrolní část

např. $\mathcal{K}_1$, $\mathcal{K}_3$ — syst.; $\mathcal{K}_2$ — nesyst.

chyby: vektor chyb $\boxed{e = b \oplus c}$
$c = b \oplus e \iff b = c \oplus e$
zjišťování chyby: $c \notin B$
oprava chyby: c nahradit „nejpodobnějším“ b
Př.: $\mathcal{K}_3$ c = 1 0 1 1 1 $\notin \{\alpha, \beta, \gamma, \delta\}$
b = 1 0 1 0 1 $= \gamma \implies$ d=10
e = 0 0 0 1 0

detekční kód — detekce (zjištění) chyby
samoopravný kód — korekce (oprava) chyby
bezpečnostní kód — detekční / samoopravný kód

Hammingova vzdálenost:

1 *slov* b' a b": vzd(b',b") — počet odlišných bitů

Př.: $\mathcal{K}_3$

	β	γ	δ
α	3	3	4
β		4	3
γ			3

2 *kódu* — kódová vzdálenost
— $kvzd$ = min vzd(b',b")
např. pro $\mathcal{K}_3$: $kvzd$= 3

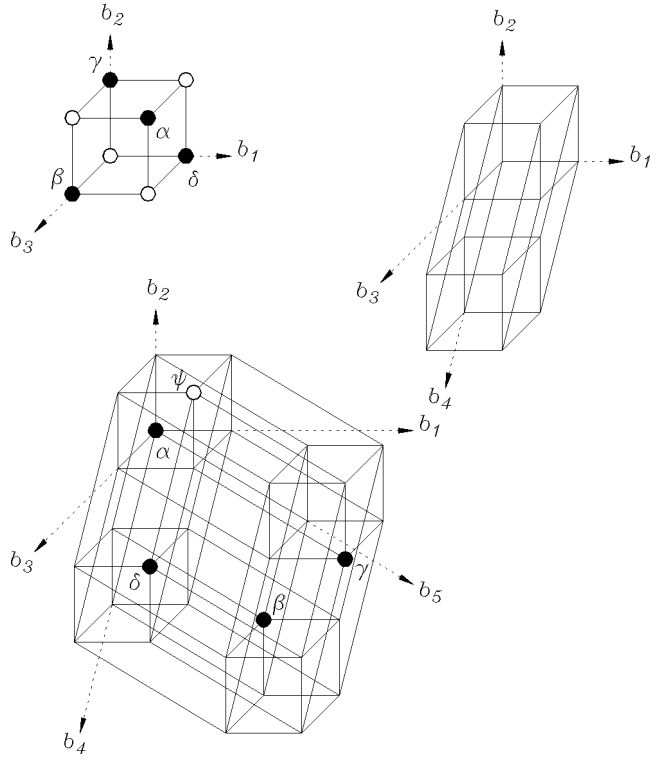
■

váha slova — počet jedniček
Př.: $\mathcal{K}_3$

α	β	γ	δ
0	3	3	4

$\boxed{\text{vzd}(b', b'') = \text{váha}(b' \oplus b'')}$

geometrická interpretace vzdálenosti:



detekce: $\boxed{dch < kvzd}$

dch ... detekovatelné chyby

oprava: $\boxed{dch + och < kvzd}$

och ... opravitelné chyby

$och \leq dch$

Př.: $kvzd = 4$

dch / och	3 / 0	2 / 1
1 ch.	D	K
2 ch.	D	D
3 ch.	D	#
4 ch.	N	N

D — detekce (bez korekce)
K — korekce
N — nic
— špatná korekce

S E D
↓ ↓ ↓
Detecting
Correcting
Error

Single
Double
Triple
Quadruple

$kvzd$	
2	SED
3	SEC nebo DED
4	SEC-DED nebo TED
⋮	

Jednoduché bezpečnostní kódy

1 *opakovací kód* $(n, 1)$:

$b_1 = \ldots = b_n = a_1$ $\qquad kvzd = n$

velká redundance $\Longrightarrow$ malý informační obsah

2 *„koktavý“ kód* (jk, k):

$j$krát se opakuje totéž (k bitů)

velká redundance $\Longrightarrow$ malý informační obsah

3 *parita* $(k+1, k)$:

$\underline{b} = (a_1, \ldots, a_k, p)$

parita $\begin{cases} \text{sudá: } p = a_1 \oplus \cdots \oplus a_k \\ \text{lichá: } p = a_1 \oplus \cdots \oplus a_k \oplus 1 \end{cases}$

minimální redundance × pouze detekce 1 chyby

4 *příčná a podélná parita*:

Př.: $k = 4 = 2 \times 2$

a_1	a_2	p_1
a_3	a_4	p_2
p_3	p_4	

$kvzd = 3$

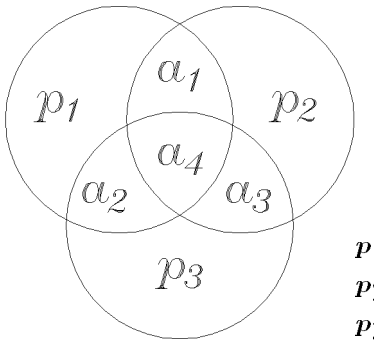
kód (8,4)

a_1	a_2	p_1
a_3	a_4	p_2
p_3	p_4	p_5

$kvzd = 4$

kód (9,4)

jeden Hammingův kód — kód (7,4)



$p_1 = a_1 \oplus a_2 \oplus a_4$
$p_2 = a_1 \oplus a_3 \oplus a_4$
$p_3 = a_2 \oplus a_3 \oplus a_4$

$kvzd = 3 \Longrightarrow$ SEC (nebo DED)

b_1	b_2	b_3	b_4	b_5	b_6	b_7
a_1	a_2	a_3	a_4	p_1	p_2	p_3

b_1	b_2	b_3	b_4	b_5	b_6	b_7
p_1	p_2	a_1	p_3	a_2	a_3	a_4
			x	x	x	x
	x	x			x	x
x		x		x		x

$$\begin{array}{lcl} b_1 & = & a_1 \oplus a_2 \oplus a_4 \\ b_2 & = & a_1 \oplus a_3 \oplus a_4 \\ b_3 & = & a_1 \\ b_4 & = & a_2 \oplus a_3 \oplus a_4 \\ b_5 & = & a_2 \\ b_6 & = & a_3 \\ b_7 & = & a_4 \end{array}$$

$$\begin{array}{lcl} b_1 & = & b_3 \oplus b_5 \oplus b_7 \\ b_2 & = & b_3 \oplus b_6 \oplus b_7 \\ b_4 & = & b_5 \oplus b_6 \oplus b_7 \end{array}$$

žádná chyba $\Longrightarrow c_i = b_i$

např.: $c_1 = c_3 \oplus c_5 \oplus c_7$

$\Longrightarrow c_1 \oplus c_3 \oplus c_5 \oplus c_7 = 0$

$$\begin{array}{lcl} s_3 & = & c_1 \oplus c_3 \oplus c_5 \oplus c_7 \\ s_2 & = & c_2 \oplus c_3 \oplus c_6 \oplus c_7 \\ s_1 & = & c_4 \oplus c_5 \oplus c_6 \oplus c_7 \end{array}$$

e	s
0000000	000
1000000	001
⋮	⋮
0000010	110
0000001	111

$$\underline{\mathbf{b}} = \underline{\mathbf{a}} \cdot \underline{\mathbf{G}}$$

$$\underline{\mathbf{G}} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

generovací matice

$$\underline{\mathbf{s}} = \underline{\mathbf{c}} \cdot \underline{\mathbf{H}}^{\mathrm{T}}$$

$$\underline{\mathbf{H}} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

kontrolní matice

Řádky každé z matic tvoří bázi tzv. vektorového neboli **lineárního prostoru.**

domácí úkol: **Najděte generovací a kontrolní matici pro dříve uvedené kódy!** Pro lichou paritu a pro kód $\mathcal{K}_2$ by se Vám to však nemělo podařit.

Má vůbec smysl používat bezpečnostní kódy ???

- **SED:** polovina chyb ???
- **SEC:** n z $2^n - 1$ chyb ???

⋮ ⋮ ⋮ ???

Pravděpodobnost:

P ... pravděpodobnost výskytu chybného bitu

n bitů i chybných: $\binom{n}{i} \cdot P^i \cdot (1-P)^{n-i}$

jinak: $\sum$

Př.: $P = 10^{-9}$ 32b / 1μsec

nějaká chyba: $32 \cdot 10^{-9}$ ... 31 sec

SED (33,32):

nějaká chyba: $33 \cdot 10^{-9}$

sudý počet chyb: $5{,}3 \cdot 10^{-16}$ ... 61,3 roků

SEC (38,32):

nějaká chyba: $38 \cdot 10^{-9}$

neopravitelná chyba: $7 \cdot 10^{-16}$ ... 46,0 roků

vektorový / lineární prostor

množina všech slov dvojkového blokového kódu
& operace:

vektorový neboli **lineární prostor V**
se skalárním součinem
nad tělesem GT(2)

- **Galoisovo (konečné) 2prvkové těleso** [field]

GT(2)

{0,1}

+	0	1
0	0	1
1	1	0

XOR

·	0	1
0	0	0
1	0	1

AND

$x+t=y \Leftrightarrow x=y+t \implies$ odčítání ≡ sčítání

- $t \in \mathrm{GT}(2)$ ⋯ skalár
- $\underline{\mathbf{v}} = (v_1, \ldots, v_n) \in V$ ⋯ vektor
- operace:
  součet vektorů — Abelova (komutativní) grupa
  násobení vektoru skalárem: $\mathbf{0} \cdot \underline{\mathbf{v}} = \underline{\mathbf{0}}$
  $\mathbf{1} \cdot \underline{\mathbf{v}} = \underline{\mathbf{v}}$
  - asociativní zákon: $(s \cdot t) \cdot \underline{\mathbf{v}} = s \cdot (t \cdot \underline{\mathbf{v}})$
  - distributivní zákony: $(s + t) \cdot \underline{\mathbf{v}} = s \cdot \underline{\mathbf{v}} + t \cdot \underline{\mathbf{v}}$
    $t \cdot (\underline{\mathbf{u}} + \underline{\mathbf{v}}) = t \cdot \underline{\mathbf{u}} + t \cdot \underline{\mathbf{v}}$

- **skalární součin vektorů $\underline{\mathbf{u}}$ a $\underline{\mathbf{v}}$:**
  $(u_1, \ldots, u_n) \cdot (v_1, \ldots, v_n) = u_1 v_1 + \cdots + u_n v_n$
  př: 01011 · 11101 = 0+1+0+0+1 = 0
- **ortogonální vektory:** $\underline{\mathbf{u}} \perp \underline{\mathbf{v}} \Leftrightarrow \underline{\mathbf{u}} \cdot \underline{\mathbf{v}} = 0$
  př: 01011 ⊥ 11101

Podprostor W prostoru V:
- $W \subset V$
- uzavřenost

Podprostor W je sám prostorem.

- **Všechny lineární kombinace vektorů $\underline{\mathbf{u}}, \ldots, \underline{\mathbf{v}}$ tvoří vektorový** (lineární) **prostor.**
- **Vektory lineárně nezávislé $\implies$ báze** (prostoru)
- **Stejný počet vektorů každé báze → dimenze**

***ortogonální doplněk U* k prostoru V: $U \perp V$**

$\underline{\mathbf{u}} \in U \iff (\forall \underline{\mathbf{u}} \in U)\ (\forall \underline{\mathbf{v}} \in V)\ \ \underline{\mathbf{u}} \perp \underline{\mathbf{v}}$

- **U je prostor, tzv. nulový prostor prostoru V**
- $U \perp V \iff V \perp U$
- **ortogonalita prostorů $\iff$ ortogonalita bází**
- $\underline{\mathbf{v}} \in V \iff (\forall \underline{\mathbf{u}} \in U)\ \ \underline{\mathbf{u}} \perp \underline{\mathbf{v}}$

Lineární kódy

kódová slova tvoří lineární prostor
popis lineárních kódů: matice
***grupové kódy* — dvojkové (?) lineární kódy**

$\underline{\mathbf{b}} = \underline{\mathbf{a}} \cdot \underline{\mathbf{G}} = a_1 \cdot \underline{\mathbf{g}}_1 \oplus \cdots \oplus a_k \cdot \underline{\mathbf{g}}_k$
$\underline{\mathbf{b}}$ = lin. komb. $\underline{\mathbf{g}}_1, \ldots, \underline{\mathbf{g}}_k$ $\underline{\mathbf{g}}_i = i$tý řádek $\underline{\mathbf{G}}$
všechna $\underline{\mathbf{b}} = \underline{\mathbf{a}} \cdot \underline{\mathbf{G}}$ → lineární prostor
báze: $\underline{\mathbf{g}}_1, \ldots, \underline{\mathbf{g}}_k$
řádky $\underline{\mathbf{G}}$ lin. nezávislé (Proč?)
$\underline{\mathbf{G}}$ → prostor V
$\underline{\mathbf{H}}$ → prostor U $\impliedby$ $V \perp U$
řádky $\underline{\mathbf{H}}$ lin. nezávislé (Proč?)

$$\underline{\mathbf{G}} \cdot \underline{\mathbf{H}}^{\mathrm{T}} = \underline{\mathbf{0}}$$

$\underline{\mathbf{G}}$: $k \times n$, $\underline{\mathbf{H}}$: $m \times n$ $\implies$ $m + k = n$

$\underline{\mathbf{c}} \in V \iff (\forall \underline{\mathbf{u}} \in U)\ \underline{\mathbf{c}} \cdot \underline{\mathbf{u}} = 0$
$\underline{\mathbf{c}} \in V \iff \underline{\mathbf{c}} \cdot \underline{\mathbf{H}}^{\mathrm{T}} = \underline{\mathbf{0}}$

$\underline{\mathbf{b}} = \underline{\mathbf{a}} \cdot \underline{\mathbf{G}}$ $\underline{\mathbf{b}} \cdot \underline{\mathbf{H}}^{\mathrm{T}} = \underline{\mathbf{a}} \cdot \underline{\mathbf{G}} \cdot \underline{\mathbf{H}}^{\mathrm{T}} = \underline{\mathbf{0}}$
$\underline{\mathbf{s}} = \underline{\mathbf{c}} \cdot \underline{\mathbf{H}}^{\mathrm{T}}$ $\underline{\mathbf{c}} = \underline{\mathbf{b}} + \underline{\mathbf{e}}$

$\underline{\mathbf{s}} = \underline{\mathbf{e}} \cdot \underline{\mathbf{H}}^{\mathrm{T}}$ $\implies$ **syndrom závisí pouze na chybě**

chyba v pozicích	$\underline{\mathbf{e}}$	$\underline{\mathbf{s}}^{\mathrm{T}}$
i	0…010…0	i-tý sloupec $\underline{\mathbf{H}}$
i a j	0…010…010…0	i-tý + j-tý sloupec $\underline{\mathbf{H}}$
⋮	⋮	⋮

ξ = počet lin. nezávislých sloupců matice $\underline{\mathbf{H}}$

ξ	dch	$kvzd$
1	1	2
2	2	3
3	3	4
⋮	⋮	⋮

$kvzd = \xi + 1$

$\underline{G} = (\underline{I}_k, \underline{F})$
$\underline{H} = (\underline{F}^{\mathrm{T}}, \underline{I}_m)$

systematický kód

$\underline{I}_j$ ...jednotková matice $j \times j$

elementární operace s řádky:

- **záměna řádků**
- **přičtení lineární kombinace jiných řádků**
- (násobení řádku nenulovým skalárem)

$\underline{G} \to \underline{G}'$ **táž množina kódových slov**
$\underline{H} \to \underline{H}'$ **jiná (vyhovující) kontrolní matice**
!!! syndromy mají jiný „význam“ !!!

$\underline{G} = \cdots \quad \underline{H} = ?$
$\underline{H} = \cdots \quad \underline{G} = ?$
} **elementární operace + + výše uvedené vztahy**

■

Nelze-li $\Uparrow$:

- **permutace sloupců**
- **nalezení matice**
- **opačná permutace sloupců**

Př.:

oprava 1 chyby $\Longrightarrow$ vzájemně různé sloupce $\underline{H}$:

$$\underline{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

elemententární operace: $1 + 2 \to 1'$
$3 + 1' \to 3'$
$2 + 3' \to 2'$

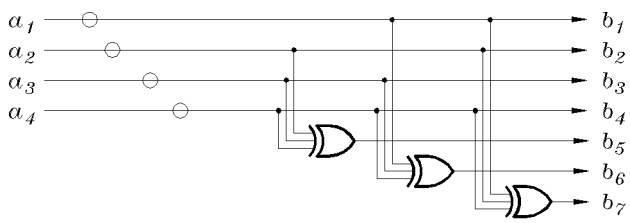
$$\underline{H}' = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

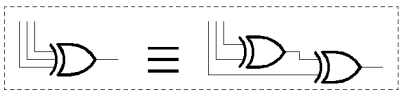
$$\underline{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Hammingův kód (7,4) — trochu jiný

kodér

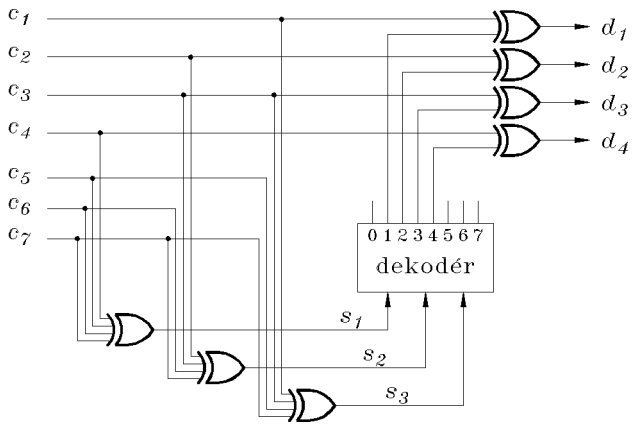
$$\underline{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$





dekodér

$$\underline{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$



kódová vzdálenost:

vzd(**b**',**b**") = váha(**b**' $\oplus$ **b**")

lin. kód $\Longrightarrow$ **b**' $\oplus$ **b**" je kódové slovo

lin. kód $\Longrightarrow$ $kvzd$ = minim. váha $\neq 0$

lin. kód $\mathcal{K}$ — lichá kódová vzdálenost

lin. kód $\mathcal{K}^*$ — kód $\mathcal{K}$ + parita (sudá)

$$kvzd(\mathcal{K}^*) = kvzd(\mathcal{K}) + 1$$

Př.: Hamm. k.: $kvzd = 3$

Hamm. k. + parita: $kvzd = 4$

↓

rozšířený Hammingův kód

Př.: příčná a podélná parita

analogicky $kvzd$: $3 \rightarrow 4$

Hammingovy kódy

perfektní kódy SEC — všechny syndromy „využity“

$kvzd = 3$ $n = 2^m - 1$ $k = n - m$

m	2	3	4	5	...
kód	(3,1)	(7,4)	(15,11)	(31,26)	...

odvozené kódy: menší $k \Longrightarrow n$; např. kódy (12,8), (21,16), (38,32), ...

rozšířené Hammingovy kódy

kvaziperfektní kódy SEC–DED — všechny syndromy „využity“

Př.:

$$\underline{\mathbf{H}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

s = x x x **1** $\Longrightarrow$ **1 chyba**

s = x x x **0** $\Longrightarrow$ **2 chyby** (kromě **s** = 0000)

(žádná chyba)

obecně: $kvzd = 4$ $n = 2^{m-1}$ $k = n - m$

m	3	4	5	6	...
kód	(4,1)	(8,4)	(16,11)	(32,26)	...

kódy RM (Reed – Muller)

parametry: ρ a μ

jčlenné logické součiny μ proměnných (pomocných)

Př.: $\mu = 3$

	j	součiny	
${}^0\underline{G}$	0	1 1 1 1 1 1 1 1	1
${}^1\underline{G}$	1	0 0 0 0 1 1 1 1	ζ
		0 0 1 1 0 0 1 1	η
		0 1 0 1 0 1 0 1	ϑ
${}^2\underline{G}$	2	0 0 0 0 0 0 1 1	$\zeta \cdot \eta$
		0 0 0 0 0 1 0 1	$\zeta \cdot \vartheta$
		0 0 0 1 0 0 0 1	$\eta \cdot \vartheta$
${}^3\underline{G}$	3	0 0 0 0 0 0 0 1	$\zeta \cdot \eta \cdot \vartheta$

ρ	0	1	2	$\cdots$
$\underline{G}$	${}^0\underline{G}$	$\begin{pmatrix} {}^0\underline{G} \\ {}^1\underline{G} \end{pmatrix}$	$\begin{pmatrix} {}^0\underline{G} \\ {}^1\underline{G} \\ {}^2\underline{G} \end{pmatrix}$	$\cdots$

$\boxed{kvzd = 2^\mu - \rho}$ $\quad n = 2^\mu$

k = **počet řádků** $\underline{G}$

Př.: RM (1, 3)

$\mu = 3, \quad \rho = 1, \quad kvzd = 4$

$n = 8, \quad k = 4, \quad$ **kód (8,4) — SEC-DED**

$$\underline{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned} b_1 &= a_1 \\ b_2 &= a_1 + a_4 \\ b_3 &= a_1 + a_3 \\ b_4 &= a_1 + a_3 + a_4 \\ b_5 &= a_1 + a_2 \\ b_6 &= a_1 + a_2 + a_4 \\ b_7 &= a_1 + a_2 + a_3 \\ b_8 &= a_1 + a_2 + a_3 + a_4 \end{aligned}$$

$$\begin{aligned} a_4 &= b_1 + b_2 = b_3 + b_4 = \\ &= b_5 + b_6 = b_7 + b_8 \\ a_3 &= b_1 + b_3 = b_2 + b_4 = \\ &= b_5 + b_7 = b_6 + b_8 \\ a_2 &= b_1 + b_5 = b_2 + b_6 = \\ &= b_3 + b_7 = b_4 + b_8 \end{aligned}$$

příklad – pokračování

$\underline{a} = (a_1, a_2, a_3, a_4) = ({}^0\underline{a}, {}^1\underline{a})$, kde

${}^0\underline{a} = (a_1)$ a ${}^1\underline{a} = (a_2, a_3, a_4)$

$$\underline{b} = \underline{a} \cdot \underline{G} = ({}^0\underline{a}, {}^1\underline{a}) \cdot \begin{pmatrix} {}^0\underline{G} \\ {}^1\underline{G} \end{pmatrix} = {}^0\underline{a} \cdot {}^0\underline{G} + {}^1\underline{a} \cdot {}^1\underline{G}$$

$$\underline{b}' = {}^0\underline{a} \cdot {}^0\underline{G} = \underline{b} - {}^1\underline{a} \cdot {}^1\underline{G}$$

$$\underline{b}' = (b'_1, b'_2, \ldots, b'_8) = a_1 \cdot (11 \ldots 1)$$

$$\underline{b}' = (b'_1, b'_2, \ldots, b'_8) = (a_1, a_1 \ldots, a_1)$$

$$a_1 = b'_1 = b'_2 = \cdots = b'_8$$

Př.: $\rho = 2$

$$\underline{b} = \underline{a} \cdot \underline{G} = ({}^0\underline{a}, {}^1\underline{a}, {}^2\underline{a}) \cdot \begin{pmatrix} {}^0\underline{G} \\ {}^1\underline{G} \\ {}^2\underline{G} \end{pmatrix} =$$

$$= {}^0\underline{a} \cdot {}^0\underline{G} + {}^1\underline{a} \cdot {}^1\underline{G} + {}^2\underline{a} \cdot {}^2\underline{G}$$

1. Určit ${}^2\underline{a}$.
2. Určit $\underline{b}' = \underline{b} - {}^2\underline{a} \cdot {}^2\underline{G}$.
3. Určit ${}^1\underline{a}$.
4. Určit $\underline{b}'' = \underline{b}' - {}^1\underline{a} \cdot {}^1\underline{G}$.
5. Určit ${}^0\underline{a} = a_1$.

Některé kódy RM

ρ	μ	n	k	m	$kvzd$
1	4	16	5	11	8
1	5	32	6	26	16
2	5	32	16	16	8
1	6	64	7	57	32
2	6	64	22	42	16
3	6	64	42	22	8

Kódy BCH

Konečná (Galoisova) tělesa

Pro každé prvočíslo p a pro každé přirozené $j > 0$ existuje právě jedno konečné těleso GT(p^j), které má p^j prvků. !!! Jiná konečná tělesa neexistují.

Př.: GT(4) = GT(2^2)

+	♢	♡	♣	♠
♢	♢	♡	♣	♠
♡	♡	♢	♠	♣
♣	♣	♠	♢	♡
♠	♠	♣	♡	♢

·	♢	♡	♣	♠
♢	♢	♢	♢	♢
♡	♢	♡	♣	♠
♣	♢	♣	♠	♡
♠	♢	♠	♡	♣

např.: $♣ + ♡ = ♠$ nebo $♣ \cdot ♡ = ♣$

♢ ... nula (♢ = 0)

♡ ... jednička (♡ = 1)

V každém konečném tělese existuje primitivní prvek α, tzn. takový prvek α, že $(\forall \beta \neq 0)\ (\exists i)\ \beta = \alpha^i$

Př.: $\alpha' = ♣$ $\quad \alpha'' = ♠$

$♣ = ♣^1 = ♣$ $\quad ♠ = ♠^1 = ♠$

$♠ = ♣^2 = ♣ \cdot ♣$ $\quad ♣ = ♠^2 = ♠ \cdot ♠$

$♡ = ♣^3 = ♣ \cdot ♣ \cdot ♣$ $\quad ♡ = ♠^3 = ♠ \cdot ♠ \cdot ♠$

Př.:

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

·	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

$\alpha = 10 = \alpha'$ (lze však použít také α''=11)

$\alpha^1 = 10$ $\quad \alpha^2 = 11$ $\quad \alpha^3 = 01 = \alpha^0$

Sčítání: XOR např.: 10+11=01

Násobení: $\alpha^i \cdot \alpha^j = \alpha^{i+j}$, např.

$10 \cdot 11 = \alpha^1 \cdot \alpha^2 = \alpha^3 = \alpha^0 =$

$= 01$

Př.: GT(16) = GT(2^4)

i	α^i	i	α^i	i	α^i	i	α^i
0	0 0 0 1	4	0 0 1 1	8	0 1 0 1	12	1 1 1 1
1	0 0 1 0	5	0 1 1 0	9	1 0 1 0	13	1 1 0 1
2	0 1 0 0	6	1 1 0 0	10	0 1 1 1	14	1 0 0 1
3	1 0 0 0	7	1 0 1 1	11	1 1 1 0	15	0 0 0 1

kódy BCH

(Bose – Chaudhuri – Hoquenghem)

(zjednodušeno)

kódy (n,k) pro opravu t chyb (tj. kód t EC)

$n = 2^\nu - 1$ a $m = n - k$

α je primitivní prvek tělesa GT(2^m)

$\underline{H} = \begin{pmatrix} \alpha^1 & \alpha^2 & \cdots & \alpha^n \end{pmatrix}$ $\quad kvzd = 3$ ... SEC

$\underline{H} = \begin{pmatrix} \alpha^3 & \alpha^6 & \cdots & \alpha^{3n} \\ \alpha^1 & \alpha^2 & \cdots & \alpha^n \end{pmatrix}$ $\quad kvzd = 5$ ... DEC

$\underline{H} = \begin{pmatrix} \alpha^5 & \alpha^{10} & \cdots & \alpha^{5n} \\ \alpha^3 & \alpha^6 & \cdots & \alpha^{3n} \\ \alpha^1 & \alpha^2 & \cdots & \alpha^n \end{pmatrix}$ $\quad kvzd = 7$ ... TEC

$\vdots$

Př.: $n = 31 \Longrightarrow$ GT(32) $\Longrightarrow$ „5bitové“ prvky

$kvzd = 3 \Longrightarrow m = 5 \Longrightarrow$ kód (31,26)

$kvzd = 5 \Longrightarrow m = 10 \Longrightarrow$ kód (31,21)

atd.

Pozn.: Uvedená kódová vzdálenost je tzv. zaručená.

Skutečná kódová vzdálenost může být větší.

Př.: kód(15,7)

$$\underline{H} = \begin{pmatrix} 1111 & 0111 & 1011 & 110 \\ 0101 & 0010 & 1001 & 010 \\ 0011 & 0001 & 1000 & 110 \\ 0001 & 1000 & 1100 & 011 \\ 0010 & 0110 & 1011 & 110 \\ 0100 & 1101 & 0111 & 100 \\ 1001 & 1010 & 1111 & 000 \\ 0001 & 0011 & 0101 & 111 \end{pmatrix}$$

Rozšířené kódy BCH

parita navíc $\Rightarrow$ oprava t chyb $\subset$ detekce t+1 chyb

(srov. rozšířený Hammingův kód)

Některé rozšířené kódy BCH

$kvzd$	n	k	n	k	n	k
6	16	7	32	21	64	51
8	16	5 (!)	32	16	64	45
10					64	39
12			32	11 (!)	64	36 (!)
14					64	30 (!)
16			32	6 (!)	64	24 (!)
22					64	18 (!)
24					64	16 (!)
28					64	10 (!)
32					64	7 (!)

Kódy a mnohočleny

mnohočleny **nad tělesem GT(2):**

Př.: $C(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$

$c_i \in$ **GT(2)** $\quad x \in ?$ ← !!!

Mnohočleny stupně $< n$**:**

- **vektorový/lineární prostor**
  (bez skalárního součinu)
- **izomorfní s prostorem uspořádaných** n**tic:**
  $c_{n-1}x^{n-1} + \cdots + c_0 \quad \sim \quad (c_{n-1}, \ldots, c_0)$
  př.: $n = 7 \qquad x^5+x^3+x+1 \sim$ **0101011**
- **izomorfie — jen: součet & násobení skalárem**

Mnohočleny:

- **násobení a dělení mnohočlenů** — obv. postup
- **analogie s okruhem celých čísel** — dělitelnost

Násobení mnohočlenů

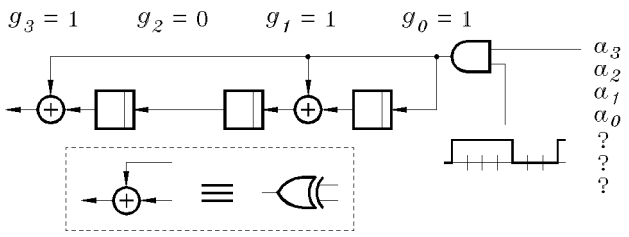
Př.: $B(x) = G(x)\cdot A(x) = (x^3+x+1) \cdot (x^3+x)$

$$\begin{array}{rl}
1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3 & G(x)\cdot x^3 \\
0\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2 & G(x)\cdot 0 \\
1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x & G(x)\cdot x \\
0\cdot x^3+0\cdot x^2+0\cdot x+0 & G(x)\cdot 0 \\
\hline
1\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x+0 & = B(x)
\end{array}$$

„zkrácený zápis“: 1 0 1 1 · 1 0 1 0

$$\begin{array}{l}
1\ 0\ 1\ 1 \\
\quad 0\ 0\ 0\ 0 \\
\quad\quad 1\ 0\ 1\ 1 \\
\quad\quad\quad 0\ 0\ 0\ 0 \\
\hline
1\ 0\ 0\ 1\ 1\ 1\ 0 \ \sim\ \underline{\mathbf{b}} = \underline{\mathbf{g}} \cdot \underline{\mathbf{a}}
\end{array}$$

(zde · **neoznačuje** skalární součin!)



Dělení mnohočlenů

Př.: $C(x) = x^6+x^2+x \quad G(x) = x^3+x+1$

$$\begin{array}{rcl}
1\cdot x^6+0\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x+0 & \Longrightarrow & 1\cdot x^3 \\
1\cdot x^6+0\cdot x^5+1\cdot x^4+1\cdot x^3 & & \hookleftarrow \\
\hline
0\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2 & \Longrightarrow & 0\cdot x^2 \\
0\cdot x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2 & & \hookleftarrow \\
\hline
1\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x & \Longrightarrow & 1\cdot x \\
1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x & & \hookleftarrow \\
\hline
1\cdot x^3+0\cdot x^2+0\cdot x+0 & \Longrightarrow & 1 \\
1\cdot x^3+0\cdot x^2+1\cdot x+1 & & \hookleftarrow \\
\hline
0\cdot x^2+1\cdot x+1 & & \\
\Downarrow & & \Downarrow
\end{array}$$

zbytek $C(x)\ \%\ G(x) = x+1$

podíl $C(x) \div G(x) = x^3+x+1 \quad \Leftarrow$

„zkrácený zápis“:

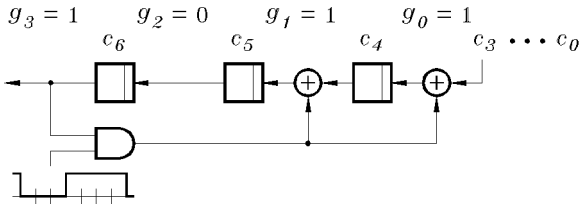
		6 5 4 3 2 1 0
$C(x)$	$\sim$	**1000110**
$G(x)$	$\sim$	**1011**
$C(x)\ \%\ G(x)$	$\sim$	**1011**
$C(x) \div G(x)$	$\sim$	**011**

Př.: $C(x) : G(x)$

$C(x) = x^6+x^2+x = c_6\,x^6 + \cdots + c_0$

$G(x) = x^3+x+1 = g_3\,x^3 + \cdots + g_0$

$$\begin{array}{l}
1\ 0\ 0\ 0\ 1\ 1\ 0 : 1\ 0\ 1\ 1 = 1\ 0\ 1\ 1 \\
\underline{1\ 0\ 1\ 1}\downarrow\ |\ | \\
\ 0\ 0\ 1\ 1\ 1\ |\ | \\
\quad \underline{0\ 0\ 0\ 0}\downarrow\ | \\
\quad\ 0\ 1\ 1\ 1\ 1\ | \\
\quad\quad \underline{1\ 0\ 1\ 1}\downarrow \\
\quad\quad\ 0\ 1\ 0\ 0\ 0 \\
\quad\quad\quad \underline{1\ 0\ 1\ 1} \\
\quad\quad\quad\ 0\ 0\ 1\ 1
\end{array}$$



Dělitelnost mnohočlenů

deg $P(x)$ — stupeň mnohočlenu $P(x)$

deg 0 $= -\infty$ (?)

deg $(P(x)\cdot G(x))$ = deg $P(x)$ + deg $G(x)$

$G(x) \neq 0$

deg $(P(x)\%G(x))$ < deg $G(x)$

deg $(P(x)\div G(x))$ = deg $P(x)$ − deg $G(x)$

$P(x)\%G(x) = 0 \iff \boxed{G(x) \mid P(x)}$

$\neq \iff \boxed{G(x) \nmid P(x)}$

$G(x) \mid P(x) \iff \exists Y(x) \quad P(x) = G(x)\cdot Y(x)$

$G(x)$ je dělitelem $P(x)$

nerozložitelný (ireducibilní) mnohočlen $P(x)$:

nemá jiné dělitele než 1 a $P(x)$ pro GT(2)!

obdoba prvočísel

rozklad na prvočinitele je jednoznačný

prvočinitel = nerozložitelný mnohočlen

Př.: $x^7 + 1 = (x^3+x^2+1)\cdot(x^3+x+1)\cdot(x+1)$

Kódy generované mnohočlenem

$$\boxed{G(x) = x^m + g_{m-1}x^{m-1} + \ldots + g_1 x + 1}$$

$m = \deg G(x) > 0$

$G(x)$ ... generovací mnohočlen

$A(x) \sim$ a ... k bitů $\implies k-1 \geq \deg A(x)$

$$\boxed{B(x) = A(x)\cdot G(x)}$$

$B(x) \sim$ b ... n bitů $\implies n-1 \geq \deg B(x)$

$$\boxed{n = k + m}$$

$m = \deg G(x)$ ... redundance

Př.: $G(x) = x^3+x+1$ a = 0101 b = 0100111

(viz př. na násobení mnohočlenů)

Pozorování: $x \mid G(x) \implies B(x) = B'(x)\cdot x$

$\implies$ b = x...x0

Závěr: musí platit $\boxed{x \nmid G(x)}$

Pozorování:

$A(x) = a_{k-1}x^{k-1} + \cdots + a_0$

$A(x)\cdot G(x) = a_{k-1}\cdot G(x)\cdot x^{k-1} + \ldots + a_0\cdot G(x)$

$G(x)\cdot x^{k-1}, \ldots, G(x)$ — lineárně nezávislé

— báze lineárního prostoru

$A(x)\cdot G(x)$ — všechny lineární kombinace

Závěr: **Kód generovaný mnohočlenem je lineární**

$$\underline{\mathbf{G}} = \begin{pmatrix} g_m & g_{m-1} & \cdots & 0 \\ 0 & g_m & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & g_0 \end{pmatrix}$$

Př.: $G(x) = x^3+x+1$

$$\underline{\mathbf{G}} = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \end{pmatrix}$$

Úkol: Ověřte, že kódy generované mnohočlenem $G(x)$ a maticí $\underline{\mathbf{G}}$ jsou stejné. Najděte kontrolní matici $\underline{\mathbf{H}}$ a všimněte si, že je to matice Hammingova kódu (7,4).

$B(x) \sim$ b ... vyslané slovo

$C(x) \sim$ c ... přijaté slovo

$E(x) \sim$ e ... chybový mnohočlen

$C(x) = B(x) + E(x)$

$\boxed{S(x) = C(x)\ \%\ G(x)}$ ... syndrom

$B(x)\ \%\ G(x) = 0$

$S(x) = E(x)\ \%\ G(x)$

syndrom závisí pouze na chybách

$E(x) = E'(x)\cdot x^j \quad x \nmid E'(x)$

$E(x)$ ... shluk chyb délky $\boxed{l = (\deg E'(x))+1}$

Př.: $E(x) \sim 0101100$ ... shluk chyb délky 4

$E'(x) \sim 01011 \quad j = 2$

deg $E'(x) = 3$

detekce chyb: $S(x) = E(x)\ \%\ G(x) = 0$?

$x \nmid G(x) \implies x^j$ nemá vliv

$E'(x)\ \%\ G(x) = 0$?

$E'(x) \neq 0$ & deg $E'(x) <$ deg $G(x) \implies$

$\implies E'(x)\ \%\ G(x) \neq 0$, tedy:

detekce shluků chyb délky $l \leq m = \deg G(x)$

Př.: $G(x) = x^{16}+1 \implies l \leq 16$

Cyklické kódy

(1) lineární kódy

(2) cyklický posuv kódového slova → kódové slovo

Př.: $\mathcal{K}_1$ — **cyklický** (viz B. k. • 2)

$\mathcal{K}_2$ — **nesplňuje (1)**

$\mathcal{K}_3$ — **nesplňuje (2)**

---

dále předp.: $G(x) \mid (x^n - 1)$, **tzn.:**

$\exists H(x)$ $\boxed{G(x) \cdot H(x) = x^n - 1}$

$H(x)$ — **kontrolní mnohočlen**
(má podstatně menší význam než kontrolní matice)

Pozorování:

$B(x) = b_{n-1}\,x^{n-1} + \cdots + b_0 = G(x) \cdot A(x)$

cykl. pos. vlevo:

$$\begin{aligned} B'(x) &= B(x)\cdot x - b_{n-1}\cdot x^n + b_{n-1} = \\ &= B(x)\cdot x - b_{n-1}\cdot (x^n - 1) = \\ &= A(x)\cdot G(x)\cdot x - b_{n-1}\cdot G(x)\cdot H(x) = \\ &= [A(x)\cdot x + b_{n-1}\cdot H(x)]\cdot G(x) \end{aligned}$$

Závěr: $\boxed{\text{Mnohočlen } G(x) \text{ generuje cyklický kód}}$

Př.: $G(x) = x^3+x+1$ $\quad G(x) \mid (x^7 - 1)$

kód (7,4) generovaný $G(x)$ je cyklický

$\mathcal{K}$ — **cyklický kód** $\implies$ $\exists\, \mathcal{K}'$:

- **kódy $\mathcal{K}$ a $\mathcal{K}'$: stejná množina kódových slov**
- **kód $\mathcal{K}'$: generován mnohočlenem $G(x)$**
- **$G(x) \neq 0$ ... nejnižší stupeň**

Př.: **kód $\mathcal{K}_1$ je cyklický** (viz B. k. • 2)

kód $\mathcal{K}_1$': $G(x) = x + 1$

táž množina kódových slov:

{ 000, 011, 101, 110 }

Systematické cyklické kódy

$B(x) = A(x) \cdot G(x)$ — **kód není systematický**
(existují výjimky)

Systematický kód:

$$\boxed{B(x) = A(x)\cdot x^m + A(x)\cdot x^m \% G(x)},$$

kde m = deg $G(x)$

Př.: $G(x) = x^3+x+1$

$A(x)$ $\sim$ **0101**

$A(x)\cdot x^3$ $\sim$ **0101000**

$A(x)\cdot x^3$ **%** $G(x)$ $\sim$ **100**

$B(x)$ $\sim$ **0101100**

!!! Množina kódových slov je u obou kódů stejná !!!

Některé cyklické kódy:

- $\underline{G(x) = x + 1}$

  $B(x) = G(x) \cdot A(x)$

  $x = 1 \implies G(x) = G(1) = 0 \implies B(x) = 0$

  $\implies B(x) = b_{n-1} + \cdots + b_0 = 0$

  $\implies$ $\boxed{\text{parita}}$ (sudá)

- $\underline{G(x) = x^m + 1}$

  $x^m \equiv 1 \mod G(x)$ ... **kongruence**
  stejný zbytek po dělení

  $C(x) = C_j(x)\cdot (x^m)^j + \cdots + C_0(x)\cdot (x^m)^0$

  $C(x) \equiv C_j(x) + \cdots + C_0(x) \mod G(x)$

  $\implies$ $\boxed{\text{„podélná“ parita } m\text{tic bitů}}$ (sudá)

- $\boxed{\text{Hammingovy kódy}}$ např.:

  $G(x) = x^3 + x + 1$ **kód (7,4)**

  $G(x) = x^4 + x + 1$ **kód (15,11)**

  $G(x) = x^5 + x^2 + 1$ **kód (31,26)**

- $\boxed{\text{BCH kódy}}$ (viz lineární kódy)

- $\boxed{\text{RS kódy}}$ **Reed – Solomon**

- $\boxed{\text{Fireovy kódy}}$

řád r mnohočlenu $P(x)$ je nejmenší takové r, že

$$P(x) \mid (x^r - 1)$$

Př.: řád x^3+x+1 je roven 7 (ale stupeň je roven 3)

$$x^i - 1 \mid x^j - 1 \iff i \mid j$$

- shluky chyb $E_1(x)$ a $E_2(x)$

  $E_1(x) = E'(x) \cdot x^i$ $\qquad x \nmid E'(x)$

  $E_2(x) = E''(x) \cdot x^j$ $\qquad x \nmid E''(x)$

  deg $E'(x)$ + deg $E''(x) < q$

  $j \geq i$

otázka: Kdy $E_1(x) \equiv E_2(x) \mod x^q+1$

úvahy: $E_1(x) - E_2(x) \equiv 0 \mod x^q+1$

$(E'(x)+E''(x) \cdot x^{j-i}) \cdot x^i \equiv 0 \mod x^q+1$

x^i neobsahuje prvočinitele x^q+1

$E'(x)+E''(x) \cdot x^{j-i} \equiv 0 \mod x^q+1$

odpověď: Právě když $E'(x) = E''(x)$ a $q \mid j-i$

- $E^*(x) = E'(x) = E''(x)$

  deg $E^*(x) <$ deg $P(x)$ a $P(x)$ má řád r

otázka: Kdy $E^*(x) \cdot (x^{j-i}+1) \equiv 0 \mod P(x)$

odpověď: Právě když $r \mid j-i$

Fireovy kódy

$P(x)$ ... nerozložitelný mnohočlen řádu r

$Q(x) = x^q+1 \rightarrow q$ a r nesoudělné $\hookleftarrow$

$p =$ deg $P(x)$ $\qquad q =$ deg $Q(x)$

$n =$ NSN (q, r) nejmenší společný násobek

$$\boxed{G(x) = P(x) \cdot Q(x)}$$

generovací mnohočlen $n$bitového Fireova kódu

$$l_1 \leq l_2 \begin{cases} l_1 + l_2 \leq q+1 \\ l_1 \leq p \end{cases}$$

detekce shluků chyb délky $\leq l_2$
oprava shluků chyb délky $\leq l_1$

Př.: $P(x) = x^3+x+1 \implies p=3 \quad r=7$

$Q(x) = x^5+1 \implies q=5 \quad q \nmid p$

$n = 35 \quad l_1 = l_2 = 3$

nebo $l_1 = 2 \quad l_2 = 4$

anebo $l_1 = 1 \quad l_2 = 5$

Prodloužené Fireovy kódy

Místo jednoho mnohočlenu $P(x)$ se použije několik mnohočlenů $P_1(x)$, $P_2(x)$, ...

Délka kódového slova: $n =$ NSN $(q, r_1, r_2, \ldots)$, kde r_1, r_2, ... jsou řády $P_1(x)$, $P_2(x)$, ...

Př.: $P_1(x) = x^{11}+x^7+x^6+x+1$

$P_2(x) = x^{12}+x^{11}+\cdots+x+1$

$P_3(x) = x^{11}+x^9+x^7+x^6+x^5+x+1$

$Q(x) = x^{22}+1$

$G(x) = P_1(x) \cdot P_2(x) \cdot P_3(x) \cdot Q(x)$

kód (558 442, 558 386), tzn. m=56

shluky délky $\leq$ 11

Oprava shluku chyb

(princip Meggittova dekodéru)

cyklický kód: $\exists H(x) \quad G(x) \cdot H(x) = x^n + 1$

$x^n = G(x) \cdot H(x) + 1$

syndrom: $S(x) = E(x)$ % $G(x)$

shluk chyb: $E(x) = E'(x) \cdot x^j \qquad x \nmid E'(x)$

$E(x) \cdot x^{n-j} = E'(x) \cdot x^n$

$E(x) \cdot x^{n-j} = E'(x) \cdot G(x) \cdot H(x) +$

$+ E'(x)$

$E(x) \cdot x^{n-j} \equiv E'(x) \mod G(x)$

$S(x) \cdot x^{n-j} \equiv E'(x) \mod G(x)$

deg $E'(x) \leq$ deg $G(x)$

$$\boxed{E'(x) = (S(x) \cdot x^{n-j}) \text{ \% } G(x)}$$

oprava: Počítá se $S(x)$, $S(x) \cdot x$, $S(x) \cdot x^2$, atd., dokud není výsledkem mnohočlen, který přísluší opravitelné chybě. Výsledný mnohočlen je roven $E'(x)$ a počet provedených kroků určuje hodnotu j.